


ORIGINAL

Approved: ROBERT W. ALLEN/DANIELLE R. SASSOON
Assistant United States AttorneyBefore: THE HONORABLE KEVIN NATHANIEL FOX
United States Magistrate Judge
Southern District of New York

17 MAG . 47 57

- - - - - X

UNITED STATES OF AMERICA

- v. -

JAMES BECKISH,
RICHARD WITCHER,
JAMES TONER,
PETER O'BRIEN, and
JOSEPH ANTHONY DEMARIA,

Defendants.

- - - - - X

: SEALED COMPLAINT: Violations of
: 18 U.S.C. §§ 1349, 1343,
: 1028A & 2: COUNTY OF OFFENSE:
: NEW YORK

:

SOUTHERN DISTRICT OF NEW YORK, ss.:

JOHN WOZNIAK, being duly sworn, deposes and says that
he is a Special Agent with United States Secret Service, and
charges as follows:COUNT ONE

(Conspiracy to Commit Wire Fraud)

1. From at least in or about 2013, up to and including at least in or about 2016, in the Southern District of New York and elsewhere, JAMES BECKISH, RICHARD WITCHER, JAMES TONER, PETER O'BRIEN, and JOSEPH ANTHONY DEMARIA, the defendants, and others known and unknown, willfully and knowingly, did combine, conspire, confederate, and agree together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343, to wit, the defendants created and operated websites that they used to place millions of dollars of unauthorized and recurring charges on credit card accounts belonging to at least tens of thousands of victims.

2. It was a part and object of the conspiracy that JAMES BECKISH, RICHARD WITCHER, JAMES TONER, PETER O'BRIEN, and JOSEPH ANTHONY DEMARIA, the defendants, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343.

(Title 18, United States Code, Section 1349.)

COUNT TWO

(Wire Fraud)

3. From at least in or about 2013 up to and including at least in or about 2016, in the Southern District of New York and elsewhere, JAMES BECKISH, RICHARD WITCHER, JAMES TONER, PETER O'BRIEN, and JOSEPH ANTHONY DEMARIA, the defendants, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, and attempting to do so, did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme and artifice, to wit, BECKISH, WITCHER, TONER, O'BRIEN, and DEMARIA, the defendants created and operated websites that they used to place millions of dollars of unauthorized and recurring charges on credit card accounts belonging to at least tens of thousands of victims, and in connection therewith and in furtherance thereof, the defendants transmitted and caused to be transmitted interstate e-mails and wire transfers of funds from the unauthorized credit card charges.

(Title 18, United States Code, Sections 1343 and 2.)

COUNT THREE

(Aggravated Identity Theft)

4. From at least in or about 2013 up to and including at least in or about 2016, in the Southern District of New York and elsewhere, JAMES BECKISH, RICHARD WITCHER, JAMES TONER, PETER O'BRIEN, and JOSEPH ANTHONY DEMARIA, the defendants, knowingly did transfer, possess, and use, without lawful authority, a means of identification of another person, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), to wit, BECKISH, WITCHER, TONER, O'BRIEN, and DEMARIA, the defendants, used and transferred, and aided and abetted the use and transfer of, the names and credit card numbers of other persons during and in relation to the charges in Counts One and Two of this Complaint.

(Title 18, United States Code, Sections 1028A(a),
1028A(b), and 2.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

5. I am a Special Agent with the United States Secret Service ("USSS"), and I have been personally involved in the investigation of this matter. This affidavit is based upon my investigation, my conversations with other law enforcement officers, victims, and companies that process online credit-card payments, and my examination of documents, including bank records and e-mail records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

Overview of the Fraud

6. As set forth in more detail below, from at least in or about 2013 through in or about 2016, JAMES BECKISH, RICHARD WITCHER, JAMES TONER, PETER O'BRIEN, and JOSEPH ANTHONY DEMARIA, the defendants, created and operated a collection of websites (the "Websites") that they used to place unauthorized and recurring charges on at least tens of thousands of victims' credit cards. The Websites purported to market and sell various products and/or services, oftentimes dietary supplements and similar products referred to as "nutraceuticals," and web

hosting services, but, in truth and in fact, the defendants used the Websites to execute a massive credit card fraud. The defendants obtained credit card numbers in bulk by buying them on the black market and by capturing the credit card numbers of individuals who sought to make legitimate purchases through the Websites. The defendants then made unauthorized and recurring charges on the victims' credit cards, oftentimes without shipping any product to the cardholders. In total, the defendants' scheme resulted in at least \$28 million in fraudulent credit card charges. Part of these illicit proceeds were routed via wire transfers to bank accounts controlled by BECKISH and WITCHER.

The Subject Companies Defraud Processor-1

7. Based on my conversations with an investigator ("Investigator-1") at a payment processing company ("Processor-1"), and my review of documents prepared by Processor-1, I have learned the following, in substance and in part:

a. Processor-1 is a credit card and debit card payment processor that processes credit card payments for millions of merchants worldwide, including online retailers. Processor-1 has offices around the world, including in Manhattan, New York. Processor-1 sometimes operates through direct business relationships with merchants. Processor-1 also partners with independent sales organizations that are responsible for generating and maintaining new merchant accounts that will use Processor-1's credit card payment processing system. One such independent sales organization that has partnered with Processor-1 is Entity-1.

b. In order for a business to register for the processing of credit card payments by its customers, a merchant must fill out a merchant processing application and agreement on which the merchant must identify, among other things, the business's website address(es), if any, as well as the corporate entity that controls the business or merchant. Once registered, a merchant will be assigned a "MID," which refers to a merchant identification number that a payment processor assigns to a merchant to process its credit card payments.

c. Processor-1 also processes "chargebacks" for the merchants that use Processor-1's services. When a customer requests and is given a refund for a credit card purchase that the customer claims was not authorized or initiated by the customer, a chargeback can be issued to the customer. A

"chargeback" is a credit, rather than a debit, that is made to the customer's credit card. Chargebacks typically arise when customers identify a charge on their billing statement for a purchase they claim not to have made. In Investigator-1's experience working for Processor-1, a chargeback rate of approximately 1% or less of all credit card purchases is typical for transactions associated with many businesses. If a business is experiencing an unusually high chargeback rate, Processor-1 may reach out to the business for an explanation or additional customer information. If a satisfactory resolution of Processor-1's chargeback concerns is not reached, Processor-1 will ordinarily close the account and stop processing credit card payments for that business.

d. Beginning in or about March 2014, Processor-1 began processing payments for a number of online retailers as a result of business generated by Entity-1. Over the course of the next year, Processor-1 began to see an increased chargeback rate for certain of these online retailers, which is a red flag for potential fraud.

e. As part of an investigation into potential fraud, in or about late 2014, Investigator-1 identified approximately 130 websites of purportedly distinct, legitimate online retailers ("the Subject Companies") that were using Processor-1's payment processing services and had average chargeback rates much higher than a typical retailer. The Subject Companies appeared to be owned and operated by the same individuals based on shared and sometimes unique characteristics, including the following:

i. The Subject Companies marketed similar products and/or services, oftentimes dietary supplements and "nutraceuticals" (products that purport to contain health-giving additives or medicinal benefit) or web hosting services.

ii. To market the products, many of the Subject Companies used identical photographs, for example a photograph of the same model holding the same product.

iii. Many of the Subject Companies used the same JavaScript coding and were hosted by the same entity.

iv. The same typographical errors appeared on many of the websites for the Subject Companies within the Subject Companies' terms of service, which were also otherwise similarly worded.

v. Many of the Subject Companies were not easily discoverable via a search engine because the words on the websites of the Subject Companies (like the company names) were not text searchable, but instead embedded in image files.

f. The average chargeback rate for transactions with the Subject Companies for the 12-month period ending on or about February 2015 was approximately 23%. The total chargebacks for the Subject Companies during that timeframe, moreover, exceeded \$8 million. Based on my training and experience investigating financial frauds, I believe that the heightened chargeback ratio is consistent with fraudulent activity on the part of the Subject Companies.

g. Due to the high chargeback rates associated with the Subject Companies and the suspicion of fraud, Processor-1 ultimately shut down its accounts with the Subject Companies. In or about January 2015, Processor-1 refunded customers a total of approximately \$28 million for credit card purchases from the Subject Companies, made while the Subject Companies had been using the payment processing services of Processor-1.

8. During the course of this investigation, I have reviewed records maintained by the Better Business Bureau and learned that over 300 complaints have been filed by consumers against certain of the Subject Companies. Many of these complaints allege, in substance and in part, that consumers' credit cards were charged for products that the consumers never ordered or that were never delivered.

9. For the reasons described below, *see infra* ¶¶ 17-20, there is probable cause to believe that the defendants operated and/or controlled the Subject Companies.

The Purchase and Use of Stolen Credit Card Data

10. Based on my investigation, I have learned that the defendants' fraudulent scheme depended on replenishing the supply of stolen credit cards that could be used to make new, and recurring, fraudulent charges. For example, based on my review of e-mails,¹ I have learned the following:

¹ As set forth below, this investigation has determined that JAMES BECKISH, RICHARD WITCHER, JAMES TONER, JOSEPH ANTHONY DEMARIA, and PETER O'BRIEN, the defendants, used the following email accounts, respectively, Beckish Account-1, Witcher Account-1, Toner Account-1, Demaria Account-1, O'Brien Account-1.

a. On or about October 21, 2013, Toner Account-1 sent an e-mail to Beckish Account-1 and Demaria Account-1, stating, "I confirmed it's about 3500 records with full info that are easily accessible and ready to go. Let me know what we can do with them, and I can help come up with a retention script as well." Beckish Account-1 responded, "Nice." Toner Account-1 subsequently responded, "I also have someone with about 1000 records from vacation clients that we can pick up for a dollar each and their average ticket was about \$500. I have made some contacts to try and acquire more as well." Based on my training and experience and participation in this investigation, I believe that in these emails JAMES TONER and JAMES BECKISH, the defendants, are discussing the purchase of credit card numbers that can then be used to make fraudulent charges, and that when TONER tells BECKISH that "their average ticket was about \$500," he means that the average amount billed by TONER's contact to each of the credit card numbers was about \$500. Based on my training and experience and participation in this investigation, I believe that TONER is telling BECKISH this information to show that the credit card numbers are creditworthy, meaning that they will not be overdrawn and will accordingly be functional, and because individuals who spend higher amounts of money per month are less likely to detect smaller fraudulent charges.

b. On or about October 21, 2013, in response to the e-mails from Toner Account-1 described *supra* ¶ 10(a), Beckish Account-1 sent an e-mail to Toner Account-1 and Demaria Account-1, that stated in substance and in part, "James please work with [Female-1] now at the call center to get a script setup for these charges. So when agents get phone calls asking what the charge is related to, we will have a good explanation. Furthermore we are going to bill them on Nutra MIDs for like \$99-\$120 per month, should have a great recurring power as well as we will try them each month." Toner Account-1 responded:

If they are just being charged under Nutra, wouldn't it be the same scripts? Or are we charging them under another model as well? If so, let me know what model and I can come up with a good script for it. We have e-mails for the majority of them so we can use that to say they opted in online for something.

Based on my training and experience and knowledge of this investigation, I understand TONER and BECKISH to be discussing how call center operators should handle customer refund requests for recurring fraudulent charges made to the MIDs of TONER's and

BECKISH's nutraceutical websites. See also *infra* ¶¶ 12-13. Specifically, TONER tells BECKISH that they "have e-mails for the majority of [the credit card owners] so we can use that to say they opted in online for something," in an effort to dissuade individuals from seeking refunds for charges they did not authorize.

c. On or about March 12, 2015, Beckish Account-1 sent Demaria Account-1 an e-mail with the subject line, "Doug Data." The e-mail's text stated, "See pricing." The e-mail included an attachment, which appears to be a screenshot of a text-message communication with "Doug" that says the following:

For 30k records plus I can do 4\$ each. I cannot go lower.
It is hard to get nowadays.
For 20k 5\$
For 15k 5.50\$
For 10k 6\$
Let me know how many u wanna start with and I will get ready for you..

These messages appear on the left-hand side of the screenshot. Based on my training and experience and participation in this investigation, I believe that JAMES BECKISH, the defendant, is arranging with JOSEPH ANTHONY DEMARIA, the defendant, for the purchase of credit card numbers from an individual who is listed in BECKISH's phone as "Doug." I know that incoming text messages generally appear on the left-hand side of commonly used smartphones, including iPhones, which the device in question appears to be.

d. On or about May 8, 2014, Witcher Account-1 sent an e-mail to another individual ("CC-1"), copying Beckish Account-1 and Demaria Account-1. The e-mail, with the subject line "No dump," stated, "Guys where is my dump for today? There's nothing in the e-mail. I need it asap to meet quotas!!!" Based on my training and experience and my knowledge of this investigation, I believe that the "dump" mentioned by Witcher Account-1 refers to fraudulent credit-card numbers that WITCHER and others can use to generate revenue by running credit card charges on their websites (that is, to "meet quotas").

The Fraudulent Credit Card Charges

11. For the reasons described below, there is probable cause to believe that JAMES BECKISH, RICHARD WITCHER, PETER O'BRIEN, JAMES TONER, and JOSEPH ANTHONY DEMARIA, the defendants, were operating multiple websites in order to make

fraudulent charges on stolen credit cards that were processed by several payment processors, including Processor-1.

12. Based on my review of e-mails, I have learned that JAMES BECKISH, JAMES TONER, and JOSEPH ANTHONY DEMARIA, the defendants, designed websites to appear like legitimate businesses in order to perpetuate the fraud. On or about October 26, 2013, for example, Toner Account-1 sent an e-mail to Beckish Account-1 and Demaria Account-1, stating in sum and substance:

Hey Guys,

Do you think we should do some things to make the website and everything look more legit? Maybe put \$1000 towards website add-ons, good reviews on various 3rd party sites, and some cheap prove-able advertising? We are pushing for these offshore accounts that can handle high volume and I just think if we do it right and make things look good, we can possibly make these merchants last longer and make it more profitable long term. What do you guys think?

Beckish Account-1 responded, in substance and part: "I agree we should use like 5% of gross to keep the site looking good or starting new sites." Demaria Account-1 then responded, asking "Hey guys, Did we get apps out?" Based on my training and experience and knowledge of this investigation, I understand BECKISH, TONER, and DEMARIA, to be discussing the operation of websites used for fraudulent merchant transactions. I believe that TONER's request to make the website "look more legit" so that "we can possibly make these merchants last longer and make it more profitable long term" reflects an effort to avoid detection by consumers and/or payment processors. BECKISH responds in agreement that they should be using money to maintain the appearance of the website, or to perpetuate the scheme by launching additional websites.

13. JAMES BECKISH and JOSEPH ANTHONY DEMARIA, the defendants, also acknowledged that they planned to charge customers without sending them any product. On or about November 11, 2015, Demaria Account-1 sent an e-mail to Beckish Account-1, stating, "Are we shipping these guys actual nutra products? lol." Beckish Account-1 responded, "Nope." And on or about May 19, 2015, Beckish Account-1 sent an e-mail to several people including Demaria Account-1 and O'Brien Account-1, stating, in substance and in part, "I think it's best if we ship healthcart [sic] type items to each person even if its just a blank letter so we have tracking. Thoughts?" Based on my training and

experience and knowledge of this investigation, I understand BECKISH to be suggesting that they create fake shipment records in order to conceal the fraud and preserve the appearance that their websites actually sell nutraceutical products, without actually sending customers any product.

14. On or about February 9, 2014, Beckish Account-1 sent an e-mail to Demaria Account-1, CC-1, and another co-conspirator not named as a defendant herein ("CC-2"), stating: "[CC-2] you need to be importing and running the data we got yesterday. It has full CVV." In a follow up e-mail to Demaria Account-1 and CC-1 on February 10, 2014, Beckish Account-1 further stated in substance and in part, "Lets setup [Entity-1] MIDS to start taking on our CCVerify CVV transactions at like 20 per day per MID and start shipping out bottles from MoldingBox (do the Colon Cleanse). We need tracking on them so pay the extra per shipment please." Based on my training and experience, I understand that "CVV" refers to a credit card verification code, usually found on the back of an actual credit card, meant to prevent fraud. I understand JAMES BECKISH, the defendant, to be telling ANTHONY DEMARIA, the defendant, CC-2, and CC-1, that he has purchased additional stolen credit card data for them to import and use, and that the inclusion of CVV data increases the likelihood that any fraudulent charges will be approved. Moreover, BECKISH appears to be telling DEMARIA and CC-1 to set up MIDS (or merchant identification numbers) with Entity-1 before running fraudulent charges on the newly purchased credit card data, and when running the charges to ship out a product chosen at random (bottles of the "Colon Cleanse") to make the transactions appear legitimate in the event of any inquiries from the payment processor.

15. Based on my investigation, I have learned that JAMES BECKISH, RICHARD WITCHER, JAMES TONER, PETER O'BRIEN, and JOSEPH ANTHONY DEMARIA, the defendants, schemed about how, when running fraudulent credit card charges in bulk, to avoid too many chargebacks that would raise red flags with payment processors. Specifically, based on my review of e-mails, I have learned the following, in substance and in part:

a. On or about September 19, 2013, Beckish Account-1 and Demaria Account-1 received an e-mail from CC-2, which stated, in part, that "73k processed today already, and increasing hourly, found VERY MUCH transactions with nice approval ratio" by removing "duplicates," which "will help to bring our chargeback ratio down." About a day later, CC-2 went on to explain in another e-mail sent to Beckish Account-1 and Demaria Account-1:

Not too bad so far today, \$32k in approvals only for the retries. Got \$20k approvals more queued aswell. Love this method of retrying transactions, getting more reasons and reasons aswell, so retrying is becoming a piece of cake. Outside that, got VERY GOOD NEWS, yesterday I noticed a lot of transactions did not had addresses/zip/city, I needed to get this solved, the zp database ... could not help because it did not contain the addresses, so added a[n] intelligent system to my customer detail checker, if user did not enter an address, and if user should not get a product, I am fetching just a random address out of the database based on matching zip/county, result, 695 orders processed and 290 approvals, so this system works nicely aswell.

Based on my training and experience and participation in this investigation, I believe that in this email CC-2 is telling BECKISH and DEMARIA that CC-2 has developed a new system to process a high volume of fraudulent transactions, and to add "a random address" in order to increase the approval percentages when running stolen credit card numbers where an address was otherwise lacking. Based on my training and experience investigating fraud and my participation in this investigation, I also believe that the low percentage of approvals ("695 orders processed and 290 approvals") shows that the business in question is fraudulent.

b. BECKISH, DEMARIA, and TONER structured the fraudulent credit card charges to avoid too many chargebacks. On or about April 13, 2015, Demaria Account-1 sent an e-mail to CC-2, copying Beckish Account-1, instructing that certain credit card transactions could be run, "just make sure approvals are not less than 25%." On or about March 22, 2016, Beckish Account-1 sent an e-mail to Toner Account-1 and Demaria Account-1 explaining, in part: "Anything \$3k+ has an extremely high statistic of coming back as a chargeback or refund or cancel. We need to keep at sub-\$2500, really sub-\$2000 is best as its industry standard ..." Later that day, in a response to the same e-mail thread, BECKISH added, in part: "[I]f someone needs to be refunded we need to refund them immediately. It's not a good idea to let the transaction potentially turn into a CB." Based on my training and experience and participation in this investigation, I believe that in these emails BECKISH is telling TONER and DEMARIA to avoid running unauthorized credit card charges above \$3,000, because those charges have a higher chance of being detected and resulting in a chargeback ("CB").

c. When the defendants ran charges on credit cards with incomplete customer data, they filled the gaps by inventing false customer information, particularly when questioned by a payment processor. See, e.g., *supra* ¶ 15(a). For example, on or about August 13, 2013, a payment processor ("Processor-2") asked for customer address and phone number information, as well as shipment and tracking information, which corresponded to certain recent credit card charges associated with a Subject Company website "Bestgreenteahealth.com." When made aware of this request, O'BRIEN, BECKISH, CC-1, CC-2, and an additional co-conspirator not named as a defendant herein ("CC-3") engaged in a lengthy e-mail discussion about how to manage the crisis that included the following statements over an e-mail thread:

i. On or about August 19, 2013, CC-1 said, "Wow, I've never seen this type of inquiry before. [CC-3], have you ever had to deal with this? I'm trying to figure out how to handle it, as it looks like rebill transactions." CC-2 responded, "Yes, we passed tracking id's from MoldingBox with fake dates, LOL!!! Anyway, let me know how to proceed with this one? But we got clearly a problem here ..." Based on my training and experience and knowledge of this investigation, I believe CC-2 to be suggesting that CC-2 knowingly falsified the information on tracking documents from Molding Box, which is a shipping company.

ii. On or about August 20, 2013, O'Brien Account-1 responded to CC-1: "Ok so do we have a list of addresses to match the cards? We can give them at least that info and make up the missing pieces?" Beckish Account-1 responded in substance and in part, "Peter - we are worried more so about the delivery tracking matching." On or about August 21, 2013, O'Brien Account-1 wrote, in substance and in part, "Can we get the shipping records and phone numbers as well as the other info included on the customer data dump sent over for all corps please?" CC-2 responded in sum and substance that, "There are no shipping records, like said previously, we never shipped anything" and "[n]o one ever received a product, so I am asking myself how we gonna solve the isuse [sic]? We got a serious problem here, and till now I hear only hear something about making product lable,s [sic] what will not solve anything. In my eyes, we got to ship the products now, or stop processing on this MID's, but we got to take action today?" Based on my training and experience and participation in this investigation, I understand O'BRIEN and BECKISH to be discussing their concerns about the inability to respond to Processor-2's questions

because they lacked certain customer information, like address information, to match the stolen credit card data ("customer data dump"), and lacked tracking information because customers were charged for products that were never actually shipped. CC-2 suggests that if they do not ship product immediately, they will have to stop making credit card charges to the website's merchant identification number.

iii. On or about August 20, 2013, Beckish Account-1 sent an e-mail that asked, in sum and substance, "[CC-1] please have a designer make a shipping invoice identical to the one used at Molding Box for our orders?" Shortly thereafter, CC-1 responded to this e-mail, "Confirmed: Working on a moldingbox template now." Based on my training and experience and participation in this investigation, I understand BECKISH to be suggesting that they falsify shipping documents that would appear to be from Molding Box, to conceal that no product was in fact shipped.

The Fraudulent Corporate Entities

16. As set forth in more detail below, JAMES BECKISH, the defendant, tried to conceal his common control of the Subject Companies by opening those companies under different fraudulent corporations using the identities of other, real people.

17. Based on my investigation and my review of e-mails between Beckish Account-1 and a person who served as a senior executive at Entity-1 in late 2014 and early 2015 ("Individual-1"), I have learned the following:

a. In late 2014, Processor-1 stopped processing payments for Entity-1 and its customers, in part because of the high chargeback rates of the Subject Companies. Shortly thereafter, Individual-1 exchanged several e-mails with "James Beckish," who emailed Individual-1 from Beckish Account-1. In those e-mails, among other things, Beckish—whom I believe based on the subject matter of this correspondence, use of the name James Beckish, and use of Beckish Account-1 was, in fact, JAMES BECKISH, the defendant—discussed resolving payment for some of the chargebacks. BECKISH participated in the negotiation of an agreement that Entity-1 executed on or about October 28, 2014, between Entity-1 and over 100 Corporate Entities (the "Corporate Entities") identified in the registration documents of the Subject Companies. The agreement specified that Entity-1 had incurred losses related to chargebacks associated with the merchant accounts of the Corporate Entities, which would pay

Entity-1 \$500,000 as partial payment for such losses through an entity called Global Media Processing LLC. An accounting manager at Entity-1 emailed Beckish Account-1 a copy of the executed agreement on or about October 28, 2014.

18. Based on my conversations with another USSS Special Agent participating in this investigation ("Agent-1"), I have learned that on or about May 3, 2017, Agent-1 spoke with an individual ("Individual-2") who works in the legal department of Processor-1. Individual-2 informed Agent-1 of the following, in substance and in part:

a. In or about late 2014, Processor-1 reached out to a bank ("Bank-1") that was receiving deposits from Processor-1 on behalf of some of the Subject Companies. Processor-1 asked Bank-1 to freeze the accounts associated with the Subject Companies on the suspicion of fraudulent activity. Bank-1 froze the accounts.

b. Individual-2 was then contacted on the phone by an attorney ("Attorney-1") who explained that he represented "James Beckish." According to Attorney-1, Beckish did not own the Subject Companies, but was hired as a consultant by some of the Subject Companies to help them resolve high chargeback levels. In or about late 2014, the attorney asked Individual-2, in substance and in part, to unfreeze the accounts at Bank-1.

c. In or around December 2014, Individual-2 spoke on the phone with James Beckish and Attorney-1. James Beckish explained, in substance and in part, that he was a consultant retained by certain of the Subject Companies and that the merchants that Beckish represented were independent of one another and, aside from small groupings of these merchants, they did not share common management or control. Beckish further informed Individual-2, in substance and in part, that he had no involvement with the Subject Companies while they were initially processing payments with Processor-1, but that he was hired only after Processor-1 started closing the Subject Companies' payment processing accounts. Beckish further explained, in substance and in part, that he was hired as a consultant for some of the Subject Companies in order to help persuade Processor-1 to reopen their accounts and assist in unfreezing the bank accounts at Bank-1.

d. On or about January 27, 2015, Processor-1 received a letter from Attorney-1, with James Beckish copied, which stated, in part, that "[w]e are making our final demand

that [Processor-1] immediately rescind/cancel the letter that it wrote to [Bank-1] requesting a freeze on the ... accounts" associated with some of the Subject Companies. The letter further stated, in part, that if such a cancellation letter were not sent "by the close of business on Friday, January 30, 2015, then I have been instructed to proceed with the filing of a lawsuit against [Processor-1] and [Bank-1] to compel the release of all funds." Processor-1 did not send such a letter, but Attorney-1 did not follow through on filing suit.

19. Upon initial review, the Subject Companies do not appear to be under the same corporate control. I have reviewed the registration applications for the Subject Companies submitted to Processor-1, which list different corporations as the controlling entity for the business. But although "James Beckish" told Processor-1 that the Subject Companies did not share common management or control, *see supra* ¶ 18(c), as part of my investigation, I have learned that JAMES BECKISH and RICHARD WITCHER, the defendants, controlled the Corporate Entities and kept track of which Corporate Entities to eliminate or to renew. That understanding is based, in part, on the following:

a. On or about January 7, 2015, Witcher Account-1 sent an e-mail to Beckish Account-1 and a co-conspirator not named herein ("CC-4"), with the subject line, "Corp renewals," stating in part, "we need to put together a list of corps that we're keeping or that need to be renewed. It's that time of the year. Jim thoughts please and [CC-4] can you list them all out so we see how many there are." Beckish Account-1 responded: "I need a list of corps first to find out which ones are dead already." CC-4 then replied on the same day: "Attached is a list of active corporations, divided into INC and LLC." Attached to CC-4's e-mail was an excel spreadsheet entitled "Corps-SD.xlsx," which included a list of over 200 corporate entities, many of which are among the Corporate Entities associated with the Subject Companies. On or about April 22, 2015, Witcher Account-1 responded to Beckish Account-1 and CC-4, stating: "I'm renewing the thread. Jim please advise which corps we need to keep." Beckish Account-1 responded that day, stating: "See attachment." Attached to the e-mail was an excel spreadsheet, entitled: "Corps-SD-20-Kill.xlsx." The spreadsheet included the same list of over 200 corporate entities, with the word "KILL" added next to many of the entity names. Witcher Account-1 responded: "Will do." Based on my training and experience and participation in this investigation, I understand that the word "kill" is used in this context to refer to

dissolving corporate entities associated with the Subject Companies, and WITCHER is agreeing to dissolve the corporate entities designated by BECKISH for dissolution.

b. Also on or about April 22, 2015, Beckish Account-1 emailed several individuals, including O'Brien Account-1 and Witcher Account-1, informing them: "I have developed a master kill list of Corporations, 800 numbers, Descriptor URLs, and Site URLs. We need to kill all of these at each provider. Please see attachment." The attachment was an excel spreadsheet entitled "MIDListKill-1.xlsx," which listed over 100 merchant names, corporate names, 800 numbers, and website uniform resource locators, or URLs. Another individual responded with the following plan of action: "I am going to ... [i]dentify the domains registrar for each domain and kill them" and "identify the number provider and see what I have to do to kill them, and kill them." That individual went on to explain that "[t]he only thing I can not [sic] do is the corps." In another e-mail to the same thread the following day, that individual also asked, "Peter could you please send me the corp domains? I do not have access to those documents but with the domains I can kill them." O'Brien Account-1 responded, "getting this list for you." Beckish Account-1 responded to the e-mail thread and stated, "Richard - we need to terminate all of these Incorporations and the LLCs that match them."

20. JAMES BECKISH, the defendant, maintained the appearance that he did not operate the Subject Companies by associating the Subject Companies with fake corporations that he directed to be incorporated using fake or stolen identities. The following is one example:

a. One of the Subject Companies was a website, "greenteapurebliss.com," which registered with Processor-1 under the corporate entity, Meltdown Wonder Services Inc, which is one of the Corporate Entities.

b. Based on my review of e-mails and e-mail attachments, I have learned that in or about June 2014, PETER O'BRIEN and JAMES BECKISH, the defendants, tried to fraudulently register "greenteapurebliss.com," with another payment processor ("Processor-3"). On the merchant application submitted to Processor-3 (the "Green Tea Application"), Meltdown Wonder Services Inc. was identified as the merchant's corporate entity. In addition, the application contained the personal identifying information of the purported female corporate owner of Meltdown

Wonder Services Inc. ("Owner-1"), including her name, address, and social security number.

c. In or about June 2014, Processor-3 reached out to the e-mail address provided on the Green Tea Application and asked for Owner-1 to contact Processor-3 in order to verify some of the information provided in the application.

d. On or about June 30, 2014, O'Brien Account-1 transmitted that request to several individuals, including Beckish Account-1, and wrote:

I need a female to call in for this please. they will ask you credit history for loans and previous jobs. Say "I cannot recall on the credit history; I would have to check my records" etc. For the previous jobs say you do a lot of outside consulting for various companies etc. But whoever calls will need to be able to identify the SSC, last address (which will be the DL address) and so on. We have all this info on the google doc. Please let me know who calls in to sort this out.

Beckish Account-1 responded, "We can have Maddy do this." Attached to that e-mail was a W-9 for Meltdown Wonder Services Inc., bank statements for Meltdown Wonder Services Inc for March, April, and May of 2014 (the "Meltdown Wonder Bank Statements"), an image of a blank check for the bank account of Meltdown Wonder Services Inc., and the application submitted to Processor-3 for "greenteapurebliss.com" in the name of Owner-1. Based on my training and experience and participation in this investigation, it appears that BECKISH and O'BRIEN used a fake identity (that of Owner-1) to open an account with Processor-3 and asked "Maddy" to impersonate Owner-1 in order to have the account approved and opened.

e. As part of my investigation I have reviewed bank records associated with the account number on the Meltdown Wonder Bank Statements. See *infra* ¶ 21(a)-(b). Those records indicate that the Meltdown Wonder Bank Statements provided to Processor-3 were doctored. For example, in the Meltdown Wonder Bank Statements, the beginning account balance on May 1, 2014 for Meltdown Wonder Services Inc is \$254,390.93. In the actual bank statements for that account number, the entity name is Meltdown Wonder LLC and the beginning account balance on May 1, 2014 is only \$2,973.44. Based on my training and experience, and the content of the e-mails described *supra* ¶ 20(d), it

appears that BECKISH used doctored bank statements that dramatically overstated the account balance in the bank account of Meltdown Wonder Services in an effort to make the company appear more creditworthy and persuade Processor-3 to process payments for greenteapurebliss.com.

f. Included on the "kill list" circulated by JAMES BECKISH on or about April 22, 2015, see *supra* ¶ 19(a), was "Meltdown Wonder LLC." Based on my experience with this investigation, it appears that Meltdown Wonder Services Inc was among the Corporate Entities that BECKISH eventually decided to "kill" after using it in connection with the fraudulent scheme.

Proceeds of the Scheme

21. Based on my and Agent-1's review of bank records, I have learned that proceeds of the Subject Companies were funneled to JAMES BECKISH and RICHARD WITCHER, the defendants, among others. For example, I have learned the following, in substance and in part:

a. WITCHER is the signatory of an account at TD Bank in the name of "Meltdown Wonder LLC" (the "Meltdown Wonder Account"). See *supra* ¶ 20(e). The Meltdown Wonder Account received payments from Processor-1 relating to sales associated with certain of the Subject Companies. Funds were also transferred out of the Meltdown Wonder Account to pay what appear to be chargebacks to Processor-1.

b. Between in or about October 2013 and in or about September 2014, the Meltdown Wonder Account received approximately \$325,014 from charges by the Subject Companies. Of that amount, approximately \$195,000 was transferred to another account in the name of "Global Media Processing LLC" at TD Bank (the "Global Media Account"). CC-3 is the signatory for the Global Media Account. The Global Media Account was also the account used by BECKISH and the Corporate Entities to partially pay Entity-1 for losses related to chargebacks, as described *supra* ¶ 17(a).

c. Other agents and I have identified approximately 20 additional bank accounts that received funds from Processor-1 resulting from credit card charges by the Subject Companies. The signatory on these accounts also appears to be either WITCHER or individuals I believe, based on my participation in this investigation, to be either associates or family members of WITCHER. Each of these accounts, moreover, transferred funds to

the Global Media Account. In total, approximately \$2,450,785 was transferred from the above-referenced 20 accounts to the Global Media Account (which also received funds from other sources) between in or about August 2014 and in or about January 2015.

d. Between in or about August 2014 and in or about January 2015, approximately \$6,170,000 was transferred from the Global Media Account to another account in the name of "Arrow Tip Marketing Ltd." (the "Arrow Tip Account").

22. Based on my review of e-mails, I believe that JAMES BECKISH, the defendant, controls the Arrow Tip Account. For example, on or about November 2, 2015, BECKISH sent an e-mail to another individual in which he asked whether the parent company for a new business could be "our master company in Anguilla/Curacao (Arrow Tip Marketing Ltd)." In a later e-mail sent on or about November 5, 2015, moreover, BECKISH sent corporate formation documents for a company called "Arrow Tip Marketing Ltd." to another individual.

The Defendants' E-mail Accounts

23. Based on my review of the contents of e-mail accounts, I have learned the following:

a. JAMES BECKISH, the defendant, appears to control and use the Beckish Account-1, because, among other things, the account contains e-mails with BECKISH's name and e-mail attachments with BECKISH's photograph. For example:

i. On or about December 28, 2015, Beckish Account-1 sent an e-mail containing seven photographs of BECKISH and an unidentified woman. I believe it is BECKISH in the photographs based on a comparison with the photograph on BECKISH's United States passport, which I have reviewed.

ii. On or about December 27, 2015, Beckish Account-1 sent an e-mail containing three photographs. One of these photographs, shows BECKISH alone facing a mirror and holding his mobile phone in a manner consistent with taking his own photograph. Another photograph in the same e-mail shows BECKISH with three other men, including a person who appears to be RICHARD WITCHER, the defendant, based on a comparison to the photograph on WITCHER's United States passport, which I have reviewed.

iii. On or about October 7, 2015, Beckish Account-1 received an e-mail, bearing the subject "Tickets & Parking - James Beckish 12/13," from a sales representative for the Miami Heat, stating in part: "James, Hope all is well! Tickets and parking are attached." On or about December 13, 2015, Beckish Account-1 received an e-mail, with the subject line "HEAT," containing a photograph of BECKISH with two other individuals.

b. RICHARD WITCHER, the defendant, appears to control and use the Witcher Account-1, because, among other things, the account contains e-mails with WITCHER's name and e-mail attachments with WITCHER's photograph. For example:

i. On or about March 26, 2015, Witcher Account-1 sent an e-mail containing a scan of a Florida driver's license (the "Florida License") with WITCHER's name and what appears to be WITCHER's photograph, based on a comparison with a photograph of WITCHER available in law enforcement databases.

ii. On or about September 3, 2015, Witcher Account-1 received an e-mail from an airline containing a boarding pass bearing WITCHER's name.

iii. On or about July 10, 2015, Witcher Account-1 received an electronic invoice from a storage facility in Winter Park, Florida, which is made out to WITCHER at the address on the Florida License.

c. JAMES TONER, the defendant, appears to control and use the Toner Account-1, because, among other things, the account contains e-mails with TONER's name and e-mail attachments with TONER's photograph. For example:

i. On or about June 16, 2014, Toner Account-1 received an invoice from a preparatory school in Florida, which lists JAMES TONER, the defendant, as the guardian of an enrolled student.

ii. On or about July 6, 2015, Toner Account-1 received an e-mail containing four photographs of TONER, based on a comparison with the photograph on TONER's United States passport, which I have reviewed.

iii. On or about November 14, 2015, Toner Account-1 received an e-mail confirmation for a spa reservation in the name of JAMES TONER.

d. JOSEPH ANTHONY DEMARIA, the defendant, appears to control and use the Demaria Account-1, because, among other things, the account contains e-mails with DEMARIA's name and e-mail attachments with DEMARIA's photograph. For example:

i. On or about July 28, 2015, Demaria Account-1 sent an e-mail containing a photograph of a woman and a person who appears to be DEMARIA, based on a comparison to the photograph on DEMARIA's United States passport, which I have reviewed.

ii. On or about October 29, 2015, Demaria Account-1 received an e-mail with the subject line "Scan from Mom." Attached to the e-mail is a scanned copy of the final judgement in DEMARIA's 2010 divorce proceeding in Seminole County, Florida.

iii. On or about January 16, 2016, Demaria Account-1 received an electronic order confirmation from an online retailer, which also lists DEMARIA's name and address in the "Shipping Address" field.

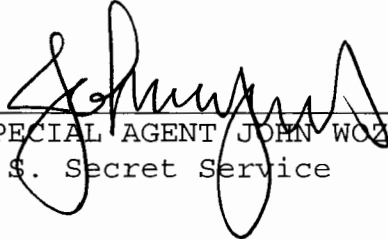
e. PETER O'BRIEN, the defendant, appears to control and use the O'Brien Account-1, because, among other things, the account contains e-mails with O'BRIEN's name and e-mail attachments with O'BRIEN's photograph. For example:

i. On or about January 12, 2016, O'Brien Account-1 sent an e-mail containing two photographs. Based on a comparison to O'BRIEN's United States passport photograph, which I have reviewed, one of these two photos appears to show O'BRIEN in a hotel room taking a photograph of himself in the mirror.


ii. On or about March 2, 2016, O'Brien Account-1 received an e-mail containing an invoice from a software provider. The invoice lists "Peter O'Brien" as the purchaser.

iii. On or about February 10, 2016, O'Brien Account-1 received an e-mail containing an electronic receipt from the North Carolina Department of Motor Vehicles for the driver's license renewal of "Peter Joseph O'Brien."

WHEREFORE, deponent respectfully requests that warrants issue for the arrests of JAMES BECKISH, RICHARD WITCHER, JAMES TONER, PETER O'BRIEN, and JOSEPH ANTHONY DEMARIA, the defendants, and that they be imprisoned or bailed, as the case may be.


SPECIAL AGENT JOHN WOZNIAK
U.S. Secret Service

Sworn to before me this
26th day of June, 2017


THE HONORABLE KEVIN NATHANIEL FOX
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK